AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1.-20. (Canceled)

21. (Original) A secure communications system including:

a first checkpoint including:

a switch including means for receipt and routing of digital information;

means for detecting the presence of secure containers;

means for determining information regarding secure containers, the information including:

a location for transmission of the secure container, and

controls associated with use or transmission of the secure container;

means for transmitting secure containers to locations designated by the secure container information, the means for transmitting capable of operating at least in part under control of controls associated with the secure containers; and

means for associating routing information with secure containers, the routing information including information indicating that the secure containers passed through the first checkpoint.

22. (Original) A system as in Claim 21, further including:

a second checkpoint adapted for communicating digital information to and from the first checkpoint, the second checkpoint including:

a switch including means for receipt and routing of digital information;

means for detecting the presence of secure containers;

means for determining information regarding secure containers, the information including:

a location for transmission of the secure container, and

controls associated with use or transmission of the secure container;

means for transmitting secure containers to locations designated by the secure container information, the means for transmitting capable of operating at least in part under control of controls associated with the secure containers; and

means for associating routing information with secure containers, the routing information including information indicating that the secure containers passed through the second checkpoint.

23. (Original) A system as in Claim 22, further including:

means at the first and second checkpoints for generating digital certificates, the digital certificates including information identifying the checkpoint which generated the certificate and including information as to the security level of the checkpoint which generated the certificate.

24. (Original) A system as in Claim 23, in which:

the first and second checkpoints are designated as having a first security level, and the system further including:

a third and fourth checkpoint, each including:

a switch including means for receipt and routing of digital information;

means for detecting the presence of secure containers;

means for determining information regarding secure containers, the information including:

a location for transmission of the secure container;

controls associated with use or transmission of the secure container;

means for transmitting secure containers to locations designated by the secure container information, the means for transmitting capable of operating at least in part under control of controls associated with the secure containers; and

means for associating routing information with secure containers, the routing information including information indicating that the secure containers passed through the checkpoint.

25. (Original) A system as in Claim 24, in which:

the third and fourth checkpoints are designated as having a second security level, which is relatively more secure than the first security level.

26. (Original) A system as in Claim 25, further including:

a secure container including governed content and at least one control specifying that the secure container must be routed through one or more checkpoints with the second security level.

27. (Original) A method of routing a secure container, the secure container including governed content and having associated a rule set at least in part governing access to or other use of the governed content, the method including:

sending the secure container from a sender to a first secure checkpoint;

at the first checkpoint, ascertaining routing information from the rule set and determining, based on the routing information, that the first secure checkpoint is authorized to receive and transmit the secure container;

at the first secure checkpoint, determining, based on the routing information, that the secure container is to be transmitted to a first recipient;

at the first secure checkpoint, associating first checkpoint information with the secure container, the first checkpoint information indicating that the secure container was received by and transmitted by the first secure checkpoint;

transmitting the secure container, including the associated first checkpoint information, to a first recipient, the transmission being governed, at least in part, by the rule set;

at the first recipient, ascertaining routing information from the rule set and determining, based on the routing information, that the first recipient is authorized to receive the secure container;

at the first recipient, determining, from the rule set, that the rule set specified a required path for transmission of the secure container from the sender to the first recipient;

at the first recipient, comparing the first checkpoint information with the specified required path; and

based on a match between the first checkpoint information and the specified required path, the first recipient undertaking an action involving the secure container.

28. (Original) A method as in Claim 27, further including:

the first checkpoint transmitting audit trail information to the sender, the audit trail information indicating that the secure container was received by the first checkpoint and transmitted by the secure checkpoint to the first recipient.

29. (Original) A method as in Claim 28, further including:

the first recipient transmitting audit trail information to the sender, the audit trail information indicating that the secure container was received by the first recipient.

30. (Original) A method as in Claim 29, in which:

the first recipient constitutes a second secure checkpoint, and the action undertaken by the first recipient includes:

ascertaining routing information from the rule set and determining, based on the routing information, that the first recipient is authorized to receive and transmit the secure container;

determining, based on the routing information, that the secure container is to be transmitted to a second recipient;

associating second checkpoint information with the secure container, the second checkpoint information indicating that the secure container was received by and transmitted by the first recipient; and

transmitting the secure container, including the associated second checkpoint information, to a second recipient, the transmission being governed, at least in part, by the rule set; and

at the second recipient, ascertaining routing information from the rule set and determining, based on the routing information, that the second recipient is authorized to receive the secure container;

at the second recipient, determining, from the rule set, that the rule set specified a required path for transmission of the secure container from the sender to the first recipient;

at the second recipient, comparing the first checkpoint information and the second checkpoint information with the specified required path; and

based on a match between the first checkpoint information, the second checkpoint information and the specified required path, the second recipient undertaking an action involving the secure container.

31. (Original) A method as in Claim 30, in which the second recipient action includes:

opening at least a portion of the secure container; and

transmitting audit trail information to the sender, the audit trail information indicating that the secure container was received by the second recipient.

32. (Original) A method including:

generating a secure container including governed contents;

associating a rule set with the secure container, the rule set including at least one rule designed to at least in part govern access to or other use of the governed contents;

associating a first digital certificate with the secure container, the first digital certificate including a digital signature;

transmitting the secure container, including the associated rule set and first digital certificate, from a first site to a first secure checkpoint;

at the first secure checkpoint, reading routing information, the routing information indicating an intended recipient of the secure container;

at the first secure checkpoint, associating a second digital certificate with the secure container, the second digital certificate including a digital signature and information evidencing the receipt of the secure container at the first secure checkpoint;

transmitting the secure container, including the associated rule set and first and second digital certificates to the intended recipient;

at the intended recipient, reading information from the first certificate and the second certificate, the information relating to the actual route taken by the secure container between the first site and the intended recipient; and

based on the actual route information, taking an action.

33. (Original) A method as in Claim 32, in which the action includes comparing the actual route information to a specified or required route.

34. (Original) A method as in Claim 33, further including:

if the comparison indicates that the actual route information is consistent with the specified or required route, accessing at least a portion of the secure container contents; and

if the comparison indicates that the actual route information is not consistent with the specified or required route, sending an indication of the inconsistency to the first site.

35. (Original) A method as in Claim 32, further including:

choosing the first secure checkpoint from at least two secure checkpoints, the choice being governed at least in part by the rule set, the choice being made prior to the transmission of the secure container to the first secure checkpoint.

36. (Original) A method as in Claim 35, in which:

the choice of the first secure checkpoint is based on an affiliation between that checkpoint and other checkpoints.

37.-41. (Canceled)

42. (Original) A secure checkpoint including:

means for receiving and transmitting secure containers, the secure containers including content and having associated a rule set designed to at least in part govern use of the content;

means for opening secure containers so as to obtain access to at least a portion of the contained content;

means for using the associated rule set to identify a required route for transmission of the associated secure container;

means for determining whether a secure container has followed the required route; and

means for associating a certificate with a secure container, the certificate including information relating to whether the secure container has followed the required route.

43. (Original) A secure checkpoint as in Claim 42, further including:

means for reviewing certificates associated with secure containers, including means for determining whether certificates have expired.

44. (Original) A secure checkpoint as in Claim 43, further including:

a memory storing a certificate revocation list and means for comparing certificates to the revocation list.

45. (Original) A secure checkpoint as in Claim 44, further including:

a directory service including information relating to electronic addresses for potential recipients of secure containers.

46. (Original) A secure checkpoint as in Claim 45, in which the directory service includes public keys of potential recipients of secure containers.

47. (Original) A network including:

a first network node including:

a secure checkpoint including means for receiving secure containers, means for reading information associated with secure containers to determine secure container routing information and means for transmitting secure containers in accordance with the routing information;

a certification authority including means for issuing digital certificates attesting to the validity of information, and means for associating certificates with secure

containers received by the secure checkpoint, the associated certificates including information indicating that the secure container was received by the secure checkpoint; and

a directory service including a memory storing address information relating to potential recipients of secure containers and means for associating recipient address information with secure containers, the recipient address information associating means being capable of operating at least in part under control of a rule set associated with the secure container.

48. (Original) A network as in Claim 47, further including:

a second network node including:

a secure checkpoint including means for receiving secure containers, means for reading information associated with secure containers to determine secure container routing information, and means for transmitting secure containers in accordance with the routing information.

49. (Original) A network as in Claim 48, further including:

a third network node including:

a secure checkpoint including means for receiving secure containers, means for reading information associated with secure containers to determine secure container routing information, and means for transmitting secure containers in accordance with the routing information; and

a fourth network node including:

a secure checkpoint including means for receiving secure containers, means for reading information associated with secure containers to determine secure container routing information, and means for transmitting secure containers in accordance with the routing information;

wherein the first network node and the second network node include a first identifier identifying them as belonging to a first web of nodes and the third network node and the fourth network node include a second identifier identifying them as belonging to a second web of nodes.

50. (Original) A network as in Claim 47, in which:

the first network node further includes means for determining whether secure containers have been received from a source consistent with the routing information, and means for transmitting a report if the secure container was not received from such a source.

51. (Original) A network as in Claim 47, in which:

the first network node further includes memory means for archiving information relating to secure containers received by the first network node secure checkpoint.

52.-71. (Canceled)